NHS
Frimley
Clinical Commissioning Group

FRIMLEY
CLINICAL COMMISSIONING GROUP

Information Governance and Cyber Incident Management and reporting Procedure

Procedure number	[Tbc by Governance team]
Version	Version 1.0
Approved by	Audit Committee in Common
Document Author	South Central West CSU
Date of approval	17 March 2021
Next due for review	1 April 2023

Version	Date	Author	Status	Comment
	16/2/2021	SCW CSU	Draft	Version adapted from East Berkshire CCG version. However, the process of reporting IG incidents described on page 8 has been standardised.

Contents

INTRODUCTION AND PURPOSE

The General Data Protection Regulation (GDPR) as implemented by the UK Data Protection Act 2018 introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority.

An organisation must notify a breach of personal data within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also inform those individuals without undue delay.

The CCG will ensure robust breach detection; investigation and internal reporting procedures are in place that complies with legislative timescales for reporting.

The CCG will also keep a record of any personal data breaches, regardless of whether it is required to notify externally.

The CCG will use the NHS Digital Data Security and Protection Incident Reporting tool Datix which is used for the purposes of notifying breaches in one central location which may then be accessed across several regulatory agencies. These include personal data breaches of the GDPR to the Information Commissioner and cyber security incidents to NHS Digital.

The CCG will comply with the Data Security Standard 6 and provide evidence of this in the Data Security and Protection Toolkit

The CCG will maintain a local file or use an incident management system to fully record the particulars of any investigation and remedial action.

The CCG recognises the importance of reporting all incidents as an integral part of its risk identification and information risk management programme through the consistent monitoring and review of incidents that result, or have the potential to result in confidentiality breach, damage or other loss.

Research has shown that the more incidents that are reported combined with the use of root cause analysis to understand why an incident has occurred, the more information will be available about any problems.

The benefits of incident and near miss reporting include:

- ✓ Identifying trends across the organization
- ✓ Pre-empting complaints
- ✓ Making sure areas of concern are acted upon
- ✓ Targeting resources more effectively
- ✓ Increasing awareness and responsiveness

Most information incidents relate to system failure and individual making mistakes or failing to follow information governance guidelines. Incident reporting needs an open and fair culture so staff feel able to report problems without fear of reprisal and know how to resolve and learn from incidents.

SCOPE

This document sets out how all information incidents, including Serious Incidents Requiring Investigations (SIRIs), will be identified, reported by staff, and managed in the CCG. It is the responsibility of all staff to ensure that personal confidential information remains secure and therefore, it is important to ensure that when incidents occur, damage from them is minimised and lessons are learnt from them.

The CCG is committed to identifying, evaluating and mitigating all risks to data subjects; these include patient/service users, permanent and temporary staff.

DEFINITIONS

Adverse Event	Any untoward occurrence which can be unfavourable and an unintended outcome associated with an incident.
Availability Breach	Unauthorised or accidental loss of access to, or destruction of, personal data.
Citizen	Any person or group of people. This would include patients, service users, the public, staff or in the context of incident reporting, anyone impacted by the incident.
Commercially confidential Data/Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Confidentiality Breach	Unauthorised or accidental disclosure of or access to personal data.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the GDPR.
Cyber Incident	There are many possible definitions of what a Cyber incident is. For the purposes of reporting, a Cyber incident is defined as anything that could (or has) compromised information assets within Cyberspace. “Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.” It is expected that the type of incidents reported would be of a serious enough nature to require investigation by the organisation. These types of incidents could include, denial of service attacks, phishing emails, social media disclosures, web site defacement, malicious internal damage, spoof website, cyber bullying.
Damage	This is where personal data has been altered, corrupted, or is no longer complete.
Destruction	This is where the data no longer exists, or no longer exists in a form that is

	of any use to the controller.
Incident	An Incident is defined as an event which has happened to, or occurred with, a patient(s), staff or visitor(s), the result of which might be harmful or potentially harmful, or which does cause or lead to injury/harm.
Integrity Breach	Unauthorised or accidental alteration of personal data.
Loss	The data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.
Near Miss	A near miss is an incident that had the potential to cause harm but was prevented. These include clinical and non-clinical incidents that did not lead to harm or injury, disclosure or misuse of confidential data but had the potential to do so.
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Personal Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the GDPR.
Serious Incident Requiring Investigation (SIRI)	There is no simple definition of a serious incident. What may first appear to be of minor importance may, on further investigation, be found to be serious or vice versa. Serious Incident Requiring Investigations (SIRIs) are incidents which involve actual or potential failure to meet the requirements of the Data Protection Legislation and/or the Common Law Duty of Confidentiality. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy. This definition applies irrespective of the media involved and includes both electronic media and paper records. When lost data is protected e.g. by appropriate encryption, so that individuals data cannot be accessed, then there is no data breach (though there may be clinical safety implications that require the incident to be reported via a different route).
'Special Categories' of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject

	(b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Unauthorised Processing	Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

ROLES AND RESPONSIBILITIES

The Accountable Officer

Has overall responsibility for Information Governance within the organisation. As Accountable Officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner for the CCG is an executive board member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at Board level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. They will oversee Serious Incidents Requiring Investigation (SIRIs).

Caldicott Guardian

The Caldicott Guardian is the person within the CCG with overall responsibility for protecting the confidentiality of personal data and special categories of personal data (described as Personal Confidential Data (PCD)) in the Caldicott 2 report, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the CCG Board and relevant committees on confidentiality issues. They will support the SIRO in overseeing Serious Incidents Requiring Investigation (SIRIs).

Data Protection Officer

The Data Protection Officer (DPO) is the person that has been assigned the responsibilities set out in the GDPR, such as monitoring and assuring CCG compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the and ICO. The DPO will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO (Information Commissioner's Office) is informed no later than 72 hours after the organisation becomes aware of the incident.

SCW Information Governance Team
The Information Governance Team will support the organisation in investigating incidents, offer advice and ensure the organisation complies with legislation, policies and protocols.

SCW Cyber Security Manager
The SCW's Cyber Security Manager will ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

Information Asset Owners (IAO)
The Information Asset Owners (IAOs) will support the organisation in investigating incidents.

Information Asset Administrators (IAAs)
Information Asset Administrators will support the organisation in investigating incidents and log any incident on their departmental Data Flow Mapping Tool.

All Staff
All staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of and comply with the requirements of this procedure.

Quality and Constitutional Standards Committee (QCSC)
The Quality and Constitutional Standards Committee is responsible for overseeing day to day Information Governance issues and provides a reporting mechanism and forum for discussing incidents, other types of IG breach and also near misses.

PROCEDURES

The procedure for reporting incidents, breaches and near misses is included as Appendix A. The online Datix Incident Reporting System can be found on the CCGs intranet site: [Datix online DIF]

TRAINING

The CCG recognises the importance of an effective training structure and programme to deliver compliance and awareness of confidentiality and data protection and its integration into day-to-day work and procedures. The identification of breaches is included in the on-line IG Training modules provided by NHS Digital that can be accessed through the Consult OD learning and development portal. Datix training sessions are also provided to CCG staff by Berkshire Healthcare NHS Foundation Trust.

MONITORING AND REVIEW

The CCG will ensure that it continually monitors its information governance structure and demonstrate it is proactive in assessing and preventing information risks by evidencing that:

a. There is continuous monitoring and improvement in confidentiality and data protection and learning outcomes;
b. All incidents are audited to ensure any recommendations made have been implemented;

c. Learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring.
d. Records of all decisions, actions, and recommendations (e.g. evidence, incident forms and reports) will be kept throughout the investigation and final report;
e. All records and documentation will be kept in a secure location;
f. Any Personal Confidential Data (PCD) including medical records, photos or other evidence will be secured at the start of the investigation;
g. File notes with dates will be kept of all discussions;
h. Minutes of all related meetings will be produced.

In line with the organisation's key documents, this document will be reviewed no later than 1 year from the date of original circulation unless new, revised legislation or national guidance necessitates an earlier review. The next review will be in April 2022.

REFERENCES AND ASSOCIATED DOCUMENTS

- Confidentiality and Safe Haven Policy
- Information Governance Staff Handbook
- Information Asset Owner and Data Custodian Handbook
- Information Governance Policy
- Data Protection Impact Assessment Guidance Framework
- Information Governance Framework and Strategy
- Information Risk Management Programme
- Records Management Policy
- SCW IT-Services Security Incident Handling Policy

The link to the NHS Digital Data Security and Protection Incident Reporting Guidance can be found here: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit

The link to the Information Commissioners Office guidance on data breaches can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

FREEDOM OF INFORMATION REQUESTS (FOI)

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management of incidents. Incidents will be defined and where appropriate kept confidential, underpinning the Caldicott principles and the regulations outlined in the Data Protection Legislation and Freedom of Information Acts.

Non-confidential incidents relating to the CCG and its services will be available to the public through a variety of means including reports, minutes and the procedures established to meet requirements in the Freedom of Information Act 2000. The CCG will follow established

procedures to deal with queries from members of the public.

APPENDIX A - STAFF GUIDANCE ON IDENTIFYING AND REPORTING AN INFORMATION INCIDENT

This guidance applies to all staff including permanent, temporary and contract staff.

All incidents must be reported to your Line Manager, Information Asset Owner and SCW IG Manager immediately you become aware of the incident.

All incidents must be reported on the CCGs online Datix Incident Reporting System within 24 hours which will automatically notify the Data Protection Officer and Information Governance Manager.

Where an incident occurs out of business hours, more serious incidents will be reported to the designated on-call officer who will ensure that action is taken to inform the appropriate contacts within 24 hours of becoming aware of the incident. This will be for example if there is a risk that a person's data rights have been seriously compromised.

What should you report?

There are three types of breaches defined under the Article 29 Working Party which informed the drafting of the General Data Protection Regulation (GDPR):

- Confidentiality breach- unauthorised or accidental disclosure of, or access to personal data

  Example - Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals. If the attacker has not accessed personal data the breach would still represent an availability breach and require notification if the potential for a serious impact on the rights and freedoms of the individual.

- Availability breach- unauthorised or accidental loss of access to, or destruction of, personal data

  Example - In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled. This is to be classified as an availability breach.

- Integrity breach - unauthorised or accidental alteration of personal data

  Example - Where a health or social care record has an entry in the wrong record (misfiling) and has the potential of significant consequences it will be considered an integrity breach. For example, a 'do not resuscitate' notice on the wrong patient record

may have the significant consequence of death whilst an entry recording the patient blood pressure may not have the same significant result.

Here are some more examples of information incidents that should be reported:

- You find a computer printout containing Confidential Data laying around;
- You Identify or are informed that a fax that was thought to have been sent to an intended recipient had been received by an unknown recipient or organisation;
- You find confidential waste in a 'normal' waste bin;
- You lose or temporarily misplace a mobile computing device or mobile phone that may have personal information on it;
- Information has been given to someone who should not have access to it – verbally, in writing or electronically;
- A computer database has been accessed using someone else's authorisation e.g. someone else's user id and password;
- A secure area has been accessed using someone else's swipe card or pin number when not authorised to access that area;
- A PC and/or programmes aren't working correctly – potentially because the device may have a virus;
- A confidential or sensitive e-mail has been sent to an unintended recipient or 'all staff' by mistake;
- A colleague's password has been written down on a 'post-it' note and found by someone else;
- A physical security breach ('break in') to the organisation is discovered;
- A phishing email has been received
- A Website has suffered from defacement

What happens next?

Where an incident involves data or information that the Controller has asked another organisation to process for them, the DPO should be informed by the Processor's Data Protection Officer of the potential breach and in addition to providing support for any necessary notification to third parties, agree an appropriate investigation plan. The same must apply where a Data Sharing Agreement has been put in place and notification of potential breaches to each party forms part of the organisations' obligations.

The incident will be investigated by the Controller but can be supported to do this by other organisations. The Controller retains the legal obligation to report and investigate incidents.

The purpose of an incident investigation is to:

- Carry out a root cause analysis in order to establish what actually happened and what actions and recommendations are needed to be taken to prevent reoccurrence;
- To identify whether any deficiencies in the application of CCG policies or procedures and/or the CCG arrangements for confidentiality and data protection contributed to the incident;

- Determine whether a human error has occurred, but not to allocate blame;
- Decide whether to notify the data subject. This decision will be made by SIRO and the Caldicott Guardian on the recommendation of the Data Protection Officer or SCW IG Manager;
- In some cases the investigation may identify whether any disciplinary processes may need to be invoked.

Assessing the severity of an incident

An initial assessment of the incident will be made using the NHS Digital Data Security and Protection Incident Reporting tool.

Notifiable breaches are those that are likely to result in a high risk to the rights of freedoms of the individual (data subject). The scoring matrix used in the reporting tool has been designed to identify those breaches that meet the threshold for notification.

The factors for assessing the severity level of incidents are determined by:

- the potential significance of the adverse **effect** on individuals graded from 1 (lowest) to 5 (highest);

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially Some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

- the **likelihood** that adverse effect has occurred graded from 1 (non-occurrence) to 5 (occurred);

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Under the following circumstances notification may not be necessary;

- Encryption – Where the personal data is protected by means of encryption.
- 'Trusted' partner - where the personal data is recovered from a trusted partner organisation. The controller may have a level of assurance already in place with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches.
- Cancel the effect of a breach - where the controller is able to null the effect of any personal data breach.

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor and the decision is taken to report the incident by the DDPO (supported by NHS England), full details will be automatically emailed to the Information Commissioners Office and the NHS Digital Data Security Centre.

Sensitivity factors have been incorporated into the grading scores and where a non ICO notifiable personal data breach involves one of the following it must still be reported as a level 2 and as such notifiable to the ICO:

- Vulnerable children
- Vulnerable adults

- Criminal convictions/prisoner information including the alleged commission of offences by the data subject or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health
- Special Categories of personal data

Assessing the risk to the rights and freedoms of a data subject

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following;

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Internal Reporting

Any information incident that takes place that is not reportable will still be included in reports circulated to the Audit Committee. These are primarily for staff awareness and to identify trends in minor incidents.

IG incident reports will also be presented to the relevant committees through the SIRO in order to provide assurance that appropriate controls are in place and that IG risks are managed effectively.

Incidents are also reported into individual teams/directorate for learning purposes and to prevent/reduce the re-occurrence.

Data Flow

The diagram below shows the flow of data when an incident is reported.